APPARATUS AND METHOD OF MAKING A SECURE CALL

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Patent Application Serial No. 60/254,462, filed December 8, 2000, which application is incorporated herein by reference in its entirety.

BACKGROUND

Field of the Invention

[0002] The invention generally relates to wireless handsets. More particularly, the invention relates to operability of handsets in non-secure and secure modes.

Background of the Invention

[0003] Security is a well-known problem in telecommunications, and in particular, wireless communications. Accordingly, handsets capable of secure or encrypted communications have been developed. However, a user of a secure handset may not always need to communicate in a secure mode, or may need to communicate with a user who does not have secure capabilities. Accordingly, what is needed is the ability for a handset to operate and smoothly transition between secure and non-secure modes of operations.

SUMMARY OF THE INVENTION

[0004] Embodiments of the invention have the ability to operate in secure and non-secure modes, and the ability to smoothly transition between secure and non-secure states. In a system of operating a wireless handset capable of making clear and secure calls, a method of making a secure call comprises pressing a key for a predetermined amount of time; entering a secure mode if the key is held for a time period greater than the predetermined amount of time; and entering a clear mode if the key is held for a time period less than the predetermined amount of time.

[0005] A wireless apparatus configurable to make clear and secure calls. The apparatus comprises a user-interface key capable of being depressed; and a time-out circuit configured to measure the amount of time the user interface key is depressed, wherein the apparatus is configured to operate in a secure mode if the user-interface key is depressed for greater than a predetermined amount of time, and wherein the apparatus is configured to operate in a clear mode if the user-interface key is depressed for less than a predetermined amount of time.

[0006] The features, objects, and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings and wherein:

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0007] Fig. 1 illustrates a typical wireless handset 100, they may optionally be provisioned with a push-to-talk button 132 and a surveillance port 136. The phone may be equipped with components such as antenna 102, earpiece 104, display icons 106, display screen 108, screen keys 110, left and right scroll keys 112, power or end key 114, down scroll key 116, clear key 118, microphone 120, far field speaker 122, message key 124, up scroll key 126, select key 128, send/talk key 130, the push-to-talk key 132, volume key 134, the surveillance port 136 and the speaker/mute button 138.

[0008] The handset is configured to operate in at least two modes:

- *Traditional:* Both clear and secure calls may be made; however, the default is preferably set for clear calls. In other words, the phone operates like a commercial phone until the user wishes to make a secure call. To place a secure call, the Send/Talk key is depressed for a predetermined amount of time.
- *Autosecure:* In autosecure mode, both clear and secure calls may be made; however, the default is for secure calls. Thus, autosecure is the opposite of traditional. While using the phone in autosecure mode, one will generally make secure calls. Thus, to make a clear call, the user depresses the Send/Talk key for a predetermined period of time.

[0009] In an embodiment, a PIN is necessary for secure calls. The PIN is an access number that is typically distributed with the phone. If the users has not previously logged on as a secure user, the user is prompted to enter the PIN when making or receiving a secure call.

[0010] Once logged on as a secure user, the user remains logged on until the phone powers down.

[0011] There are several ways to make calls:

1. Traditional, press the Send/Talk key for clear mode, press and hold the Send/Talk key for secure mode;
2. Autosecure, press and hold the Send/Talk key for secure mode, press the Send/Talk key for clear mode; and

3. Secure-Only, can only make emergency clear calls (enter 91 1, *91 1, or #91 1 and press and hold the Send/Talk key) for secure mode, press the Send/Talk key for clear mode.

[0012] Fig. 2 is a flow chart 200 illustrating determination of a clear, secure, or auto secure call. The handset first senses 204 if the SEND key is pressed and held. If not, the next inquiry 208 is whether the handset is a secure-only handset. This inquiry may not be necessary, but rather a default position setting in a secure only handset. If the handset is a secure-only handset, a request 212 for a secure call origination is sent. If the handset operates in both clear and secure modes, the next inquiry 216 is whether the handset is in auto secure mode. If the handset is in auto secure mode, a request 220 for a secure call origination is sent. If the handset is not in auto secure mode, a clear call origination 224 is requested.

[0013] If the send key is pressed and held, the next inquiry 228 is whether the handset is a secure-only handset. Again, this inquiry may not be necessary, but rather a default position setting in a secure only handset. If the handset is a secure-only handset, a request 232 for a secure call origination is sent. If the handset operates in both clear and secure modes, the next inquiry 236 is whether the handset is in auto secure mode. If the handset is in auto secure mode, a require confirmation request 240 is sent to request clear call origination. If the request 240 is not confirmed, the call may fall back into clear mode. If the handset is not in auto secure mode, a request secure call message 244 is sent.

[0014] Whenever a call is in secure mode, the call may fall back into clear mode if needed. This may occur either because the receiving party is not a secure handset, or if the parties decide to switch to clear mode.

[0015] If one is making a clear call, the phone behaves like a commercial phone, and the call is connected. If the person being called has a secure-only phone, the screen displays a message such as "GOING SECURE/Exchanging secure dial/#. . . ." If the user has not previously logged on as a secure user, the user is prompted to enter your PIN.

[0016] Fig. 3 illustrates a flowchart 300 for determining whether a secure user has logged in. First, a login prompt 304 is displayed, allowing the user to enter a PIN. If a valid PIN is entered, the user is returned to the calling process 306. If not, the user begins the PIN entry process 308. The next determination 312 is whether the PIN entry was successful. If not, the secure call request is aborted 316. A message 320 is presented indicating that the call cannot be placed without a valid PIN. The message may remain on the screen either for a predetermined amount of time, or until the user presses a key. If the PIN entry was successful, the user is returned to the calling process 324.

[0017] If the user is making a secure call and has not already entered your PIN, a message appears on the handset screen asking the user to enter it. After the PIN is entered, the phone displays a message such as "GOING SECURE" followed by a series of messages. If the user is not prompted to enter your PIN, it means the user is already logged on as a secure user.

[0018] In a phone capable of both clear and secure modes, one can switch the type of call connection *during* the call. For example, if a clear call connection is established with another party, the call may be a secure connection. The process of transitioning from a clear connection to a secure connection is illustrated in FIG. 2.

[0019] From the screen keys at the bottom of the display, select [GOSEC].

- Press and hold the Send/Talk key depending on your phone's strapping.
- Enter the PIN if prompted to do so. The person being called might also be prompted to enter a PIN. The type of messages that appear and the length of the connection time depends on whether the phone number has been previously recognized and stored as secure in the other party's phone.

[0020] Transition from secure to clear connections may be accomplished in one of the following ways:

- From the screen keys at the bottom of the display, select [GOCLR].
- Press or press and hold the Send/Talk key. A message appears on the phone display of the person called requesting confirmation to transition from secure to clear.

[0021] During a secure voice or data call, depending on the security classification, either fingerprints or DAO descriptors appear on the screen.

- Fingerprint: contains security classification (Protected = PROTEC), time, and a combination of a number of letters, numbers, or punctuation marks, which can read to the other party. The same combination may be displayed on all phones on the call. If it is not the same or the line is blank, the security of the call may be compromised. The following is a non-limiting example of a screen with a fingerprint:

DAO descriptor: contains security classification (Top Secret = TS, Secret = SEC, Confidential = CONF, and Unclassified = UNCLAS), time, and identification. The DAO descriptor is similar to caller ID and is not the same on both phones in the call.

[0022] In receiving secure calls, if one has not already entered your PIN since turning on the phone, the user is prompted to enter it. After entering the PIN, the phone displays "GOING SECURE" followed by a series of messages. The types of messages displayed and the length of the connection time depends on whether the phone number has been previously recognized and stored as secure in the calling party's phone book. When the secure call is connected, a secure call screen appears.

[0023] In originating a Point-to-Point Voice Call, typically, a user requests origination of the call. If voice calls are disabled in the UPV, the operator is alerted and call origination does not proceed. Otherwise, based on the method of call origination (long key press, short key press, one touch dialing, or two-touch dialing) and the phone's strapping (traditional, secure-only, or auto-secure), the user interface determines whether to attempt a clear or secure call. The user interface then determines the number to be dialed, in cases where both clear and secure dial numbers are available. In an embodiment, a call to an emergency number is attempted as a clear call, and go-secure transitions are not allowed.

[0024] There are at least nine ways in which a point-to-point voice call may be placed from the user interface:

1. Manually entering the phone number and pressing [SEND] or pressing and holding [SEND].
2. Selecting a number from the Call History List and pressing [SEND] or pressing and holding [SEND].
3. Recalling a number from the Call History Detail Display and pressing [SEND] or pressing and holding [SEND].
4. One Touch Dialing by pressing and holding the digit corresponding to the desired phone memory location number.
5. Two Touch Dialing by pressing and holding the digits corresponding to the desired phone memory location number. For example, to dial memory location 25, press 2 then press and hold 5.
6. Speed dialing by entering I or 2 digits and pressing [SEND] or pressing and holding [SEND].
7. Dialing from a phone book memory list by pressing [SEND] or pressing and holding [SEND].
8. Dialing from a phone book memory display by pressing [SEND] or pressing and holding [SEND].

9. Pressing [SEND] to redial from standby mode (if an outgoing call has been made and the handset has not been power cycled). The last outgoing number information is now stored in NV memory when the handset is powered off *(i.e.,* the handset can be powered off and then powered on again and the [SEND] key will still dial the last out going number).

[0025] The following logic may be used by the user interface to determine whether the user has requested clear or secure point-to-point voice call origination.

- In any mode, an emergency call is treated as a clear call origination request.
- In traditional mode, one-touch dialing, two-touch dialing, and short [SEND] key presses initiate clear voice calls. Extended [SEND] key presses initiate secure voice calls.
- In secure-only mode, requests for call initiation result in secure calls, with no fall back to clear.
- In auto-secure mode, one-touch dialing, two-touch dialing, and short [SEND] key presses initiate secure voice calls. Extended [SEND] key presses initiate clear voice calls, after user confirmation.
- In traditional and auto-secure mode, secure call initiation may revert back to a clear call if the secure call cannot be established.

[0026] If the "last outgoing number" is being dialed, the above rules still apply, regardless of whether the last outgoing number was clear or secure. The length of the key press, together with the mode of the phone, determine whether a clear or secure call has been requested.

[0027] Fig. 4 illustrates a flowchart 400 of placing a secure call. The first inquiry 404 is whether the user selected number is available in the phone book. If not, a secure, or data, call is initiated 408 to the user selected number. If the number is available in the phone book, the next inquiry 412 is whether the number is registered in the phone book as a secure number. If so, a secure call 416 is initiated to the user selected number. If not, a next inquiry 420 is made as to whether a secure number is listed in the phone book in association with the user selected number. If so, the secure number in association with the user selected number is used to initiate a call 424. If not, a clear voice call to the user selected number is initiated. This may be followed by a clear to secure transition 428, if needed.

[0028] Fig. 5 illustrates an apparatus 500 for making clear and secure calls. A user interface 504, such as a SEND button, is operable when depressed by the user. A circuit 508 determines the length of time the user depresses interface 504. If the user-interface 504 is activated for more than a predetermined amount of time, the apparatus is configured to operate in secure mode. If the user-interface 504 is activated for less than a predetermined amount of time, the apparatus is configured to operate in clear mode. In an embodiment, the predetermined amount of time is between .01 and 5 seconds. In another embodiment, the predetermined amount of time is between 1 and 3 seconds. In another embodiment, the predetermined amount of time is 2 seconds.

[0029] If the request for point-to-point voice call origination is for a secure call, a check may be made to determine whether the secure user has logged in. If the secure user has not logged in, the login prompt is presented. Successful login results in a continuation of the call origination process. Unsuccessful login (whether aborted by the user or by too many failed logins) may result in a return to an Idle Standby Mode.

[0030] The following logic may be used to determine what number should be dialed for a point-to-point voice call origination request:

[0031] When a clear call has been requested:

- If the number cannot be found in the phone book, initiate a clear voice services *call* to the user-selected number.
- If the number can be determined, from the phone book, to be a voice (clear) number, then initiate a clear voice services call to the user-selected number.
- If the number can be determined, from the phone book, to be a data (secure) number, and there is an associated voice number, then initiate a clear voice services call to the associated voice. number.

[0032] If the number can be determined, from the phone book, to be a data (secure) number, and there is no associated voice number, then initiate a clear voice services call to the user-selected number (even though it is a data number).

[0033] When a secure call has been requested:

- If the number cannot be found in the phone book, initiate secure data services call to the user-selected number.
- If the number can be determined, from the phone book, to be a data (secure) number, then initiate a secure data services call to the user-selected number.
- If the number can be determined, from the phone book, to be a voice (clear) number, and there is an associated data (secure) number, then initiate a secure data services call to the associated data number.

- If the number can be determined, from the phone book, to be a voice (clear) number, and there is no associated data (secure) number, then initiate a clear voice services call to the user-selected number, followed by an immediate clear-secure transition.

[0034] If the secure call was successfully negotiated, and the security level is commercial security (i.e., 'Protected'), the fingerprint is calculated and displayed during the call.

[0035] The fingerprint may be any number of bits. In an embodiment, the fingerprint is 48 bits, obtained from the DSP. These bits are broken down into 8 6-bit chunks. Each chunk's bits correspond to a decimal value, which corresponds to a character using the following mapping:

- 0 - 25 map to A - Z
- 26 - 51 map to a - z
- 52-61 maptoO-9
- 62 maps to +
- 63 maps to /

[0036] Both ends of the phone call should have calculated the same 48 bits, and should have the same 8 characters on their display. One user can read out his display to the other user, and they can compare to verify that there is no "man in the middle" attack.

[0037] When a clear point-to-point non-emergency call is active, the user can request a transition to a secure voice call or to a secure data call by using the appropriate soft key or by a long press of the [SEND] key. If the user has not yet logged in as the secure user, he is prompted to login before the transition request is sent (see PIN Entry Check). When the other end receives the go-secure request, the user there is prompted to log in if he has not already done so.

[0038] If the user attempts a clear to secure transition when in an emergency call, the following display may result.

[0039] When a secure point-to-point call is active, the user may request transition to a clear point-to-point call by using a soft key or by a long press of the [SEND] key. FNBDT signals the go-clear request to the other end, and the user there is prompted to confirm the go-clear transition.

[0040] If the user who is strapped for secure-only attempts a go-clear transition, the following text may be displayed for a predetermined period of time. In an embodiment, the text is displayed for about 4 seconds (or until a key press). An audible beep will sound (unless restricted), and the secure call will continue.

[0041] Secure Dial is permitted when a secure voice call has been established. The user enters digits, *, and # and then presses the [SEND] key to send the digits as a secure dial stream. The user may also activate a soft key for access to additional secure dial characters (Autovon FLASH-OV, FLASH, IN4MEDIATE, and PRIORITY, as well as Go On Hook and Hookflash). The secure dial display is a multi-page display.

[0042] The secure application mode change allows the user to change from secure voice to secure data. (When in the data mode, the user has an option to change from secure data to secure voice.) The mode change is typically valid after secure voice has been established. The mode change is requested by accessing the [DATA] soft key option from In Use Standby.

[0043] A clear data call is typically originated via a command from the communication software of a connected computing device. A clear data call cannot be directly connected from the handset keypad. A secure data call is originated by selecting the Secure Data option from the Features menu and then dialing the number from the keypad. The user is alerted if the UPV prohibits the requested data call. Unless disabled, the backlight is illuminated at initiation of a data call.

[0044] Additional notes for outgoing data calls:

[0045] Typically, no additions to the call history list will occur for outgoing clear data calls. The call history will be updated for outgoing secure data calls.

- If the last outgoing call on the handset was a clear data call (which is dialed from AT commands through the data port), then the last number redial feature (user pressing [SEND] key) will dial the last number that was dialed through the keypad.
- If no redial number is available, the following display will be shown, and the standard key beep tone will be played as applicable.

[0046] The CST typically cannot receive clear data calls. The following activity occurs upon receipt of a data call:

- Since the CST does not support unattended mode, data calls must be answered from the keypad. The determination of whether the call is for data or voice is not made until FNBDT negotiation.
- Data calls cannot be answered from the external computing device's communication software commands. A data call will be answered when the user presses [SEND], even if the keypad is locked and the keypad will remain locked through the duration of the call and at the end of the call.
- The ringer may be silenced in the standard manner.

- Typically, the phone cannot distinguish incoming secure data calls from incoming secure voice calls, since the determination of voice or data application is not made until FNBDT negotiation. Incoming secure data call behavior is therefore the same as for incoming secure voice call (the CST does not support incoming clear data calls).

[0047] The Key Management functionality requires that the user be offline. If the user is in a call when this option is selected, the "Feature not available during a phone call" display is shown.

[0048] While in the key management functions, the user is not allowed to go online (by initiating or receiving a call). While keys are being loaded, the Security Subsystem may, in addition, suspend communication with the base station by taking the modem offline.

[0049] Key management supported by the user interface allows the secure user (when the secure user PIN has been entered) to selectively delete key material, to delete all key material, and (if authorized through the UPV) to load key material.

[0050] The user will be prompted to logon (if not already logged on) when the "Load Keys" menu item is selected. The user's ability to load keys is enabled through the UPV. The implementation of this function is otherwise identical to the TA's ability to load keys.

[0051] The user will be prompted to logon (if not already logged on) when the "View Keys" menu item is selected. The user's ability to view and delete keys is otherwise identical to the TA's ability to view and delete keys.

[0052] The user will be prompted to logon (if not already logged on) when the "Delete All Keys' menu item is selected. The user's ability to delete all keys is otherwise identical to the TA's ability to delete all keys.

[0053] Those of skill in the art would understand that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. The various illustrative components, blocks, modules, circuits, and steps have been described generally in terms of their functionality,. Whether the functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans recognize the interchangeability of hardware and software under these circumstances, and how best to implement the described functionality for each particular application. As examples, the various illustrative logical blocks, flowcharts, windows, and steps described in connection with the embodiments disclosed herein may be implemented or performed in hardware or software with an application-specific integrated circuit (ASIC), a programmable logic device, discrete gate or transistor logic, discrete hardware components, such as, e.g., registers in the FIFO, a processor executing a set of firmware instructions, any conventional programmable software and a processor, a field programmable gate array (FPGA) or other programmable logic device, or any combination thereof. The processor may advantageously be a micro-controller, but in the alternative, the processor may be any conventional processor, controller, micro-controller, or state machine. The software may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, hard disk, removable disks, a CD-ROM, a DVD-ROM, registers, or any other magnetic or optical storage media. Those of skill of the art would further appreciate that the data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description are advantageously represented by voltages, currents, electromagnetic waves, magnetic field or particles, optical fields or particles, or any combination thereof.

[0054] The previous description of the preferred embodiments is provided to enable any persons skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein, but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

[0055] What we claim as our invention is: